MENACING MALWARE:

EXPOSING THREATS LURKING IN YOUR LINUX-BASED MULTI-CLOUD

special focus
An SC Media publication

Sponsored by

vmware®

Malware moving to Linux-based cloud systems

Linux-based threats are often overlooked. That's a problem since most multi-cloud environments are Linux-based. VMware recently shined a spotlight on the problem in a report and SC Media webcast.

It's a fact: Most of the cloud runs on Linux With 90% of the cloud powered by the Linux operating system, it's predictable that malware would follow — and it certainly has. But most modern security tools are designed to solve Windows-based threats.

With this evolution in mind, VMware's Threat Analysis Unit recently set out to study the growth of Linux-based malware and its threat to multi-cloud environments.

This SC Media Special Focus provides a high-level overview of VMware's findings, including the unique characteristics of Linux-based remote access tools (RATs), ransomware, and crypto-miners on Linux-based systems. Also included is guidance for how security teams can protect their organizations from Linux-based malware, ransomware, and crypto miners.

OUR EXPERTS: EXPOSING THREATS LURKING IN YOUR LINUX-BASED MULTI-CLOUD

Giovanni Vigna, Senior director of threat intelligence, VMware
Brian Baskin, Technical lead, VMware Threat Analysis Unit

"If you look at infrastructures and clouds, Linux is the most popular operating system, and it powers many of the websites that you visit every day," Giovanni Vigna, senior director of threat intelligence at VMware, said during a recent webcast and report, Menacing Malware: Exposing threats lurking in your Linux-based multi-cloud. "However, for various reasons, malware research has focused for the vast majority on Windows threats."

Growing Linux threats in multi-cloud systems

VMware researchers have witnessed attacks that target cloud infrastructure and even use cloud management tools to shut down virtualized systems so that they can encrypt systems, workloads, and data. Threat actors, such as the ransomware gang HelloKitty, moved from Windows systems to Linux by developing new versions of their software used in attacks.

"It became important for us to look more closely at these types of threats," Vigna said. "We've also seen how open Docker infrastructure and open Kubernetes infrastructure can be leveraged to deploy new [malware] components."

The rise of Linux ransomware

Ongoing ransomware attacks, at least initially, occur much like any other type of compromise. There's an initial breach, such as an exploited application or a successful phishing attack. Then attackers burrow deeper into and gain a persistent foothold in the environment. Once established, the attackers will launch a command-and-control communication line so that ransomware can be readily executed. However, rather than exfiltrating data, the attackers will encrypt data or critical systems — essentially denying access — until payment is made.

More recently, attackers have first exfiltrated the victim's data, and if the ransom isn't paid, they threaten to release that data on the dark web. The VMware research team has also witnessed ransomware attackers shifting from targeting

single installations to attacking data centers to targeting cloud workloads. "This is a worrisome trend that I'm sure will continue for the foreseeable future as the cloud becomes more and more important," Vigna said.

Part of the evolution of ransomware is its increased targeting of Linux systems. Ransomware, such as Defray777, encrypts host images on VMware ESXi servers.

In its research, VMware analyzed nine families of ransomware that target Linux systems. These families include Erebus, GonnaCry, and eCh0raix.

Giovanni Vigna, senior director of threat intelligence at VMware

The research team identified considerable code sharing by analyzing malware, including associated shell and Python scripts and binaries. This included such widespread malware as DarkSide and BlackMatter, and ViceSociety sharing code fragments with REvil.

> "If you look at infrastructures and clouds, Linux is the most popular operating system, and it powers many of the websites that you visit every day. However, for various reasons, malware research has focused for the vast majority on Windows threats."
>
> *–Giovanni Vigna, senior director of threat intelligence at VMware*

The researchers further identified the capabilities of the Linux-based ransomware and correlated them to the MITRE ATT&K framework. They found defense evasion, obfuscated files or information in 59% of the samples, system information discovery in 18%, and de-obfuscated/decoded files or information in nearly 11% of samples.

To mitigate the Linux ransomware threat, the VMware team recommends enterprises follow best security practices, including a suitable data backup and recovery process, an EDR solution, and NDR to spot attacks on the network.

Linux-based crypto miners

VMware researched crypto-mining malware with the same methodology. The process of stealing computing power, commonly referred to as "cryptojacking," is the process of infecting systems with crypto mining software and stealing system CPU resources, essentially creating a digital currency. This is a lot less risky than infecting enterprises with ransomware and then trying to extort those victims for cash.

But these attacks can be costly and result in more expensive electric bills, increased costs associated with cloud computing consumption, and will result in hits to cloud and system performance. However, because these attacks aren't as bold as capturing systems or data, they can run under the radar for a time.

Cryptojacking attacks are no stranger to cloud systems. As the report authors noted, "The first cryptojacking attacks was against Tesla's public cloud — a Kubernetes deployment was hijacked and dedicated to mining the currency, while the computational costs were paid by Tesla. This notorious event was just the first in a series of incidents that targeted the CPU cycles of cloud environments."

When VMware researchers applied their analysis to crypto miners, they found that nearly all miners utilize XMRig. Vigna said the amount of XMRig code sharing enabled the researchers to track the evolution of Linux-based mining software.

The team also examined the behaviors of the crypto mining samples they gathered. Similar to the behaviors observed in the ransomware samples, defense evasion is the most commonly used technique. Regarding the encryption methods associated with defense evasion, it appears the techniques crypto miners use to obfuscate data are more diversified.

Brian Baskin, technical lead, Threat Analysis Unit at VMware

"Also, for example, we noticed that crypto miners are not very concerned about detecting if they are on a virtualized workload, while ransomware is very active trying to evade analysis," said Vigna.

To detect and mitigate the threat, VMware researchers advise that network traffic analytics is the best way to identify crypto-jacking attacks. This will spot local hosts communicating externally. However, due to the increased use of sophisticated obfuscation techniques, it's becoming increasingly necessary to rely on endpoint detection and response tools to identify suspicious CPU usage patterns. This is why the team advises monitoring cloud environments with host- and network-based detection systems.

> "The first cryptojacking attacks was against Tesla's public cloud – a Kubernetes deployment was hijacked and dedicated to mining the currency, while the computational costs were paid by Tesla. This notorious event was just the first in a series of incidents that targeted the CPU cycles of cloud environments."
>
> *– VMware researchers*

Remote Access Trojans & Cobalt Strike

Of course, attackers don't typically attack Linux and cloud (and other) systems for the sport of it: They have an objective in mind. Whether that objective is ransomware, crypto jacking, or other goals. To do that, attackers must gain control within the environment, such as creating a staging server so they can target other networked systems and move laterally, deeper, into the organization. Such is the case with Remote Access Trojans (RATs) and other implants, which serve as ways to monitor endpoints with keyloggers, take screenshots, exfiltrate or destroy data, plant additional malware (such as ransomware), and more.

This is how attackers gain and maintain control, persistence, and further their goals.

"We have to focus on how payloads actually get into place," says Brian Baskin, technical lead for VMware's Threat Analysis Unit. Baskin explains that understanding what mechanisms adversaries use to take control of the environment and how it's activated and detonated is essential to protecting against these threats.

One of the first things RATs and other implants do is scan for other systems accessible on the network.

"They will use that one compromised machine to jump to the next machine. They will enumerate all the resources within environments, such as the operating systems and vulnerabilities, and then use whatever exploits they can to move around," says Baskin.

The attacker may scan the entire range of IP addresses, or because servers and high-value systems are often stored at the lower or higher ends of the range, attackers will scan those areas of the range. As systems

are identified, information about those systems — addresses, hostnames, active user accounts, operating systems, and software versions — are collected.

So that the attacker implant conducting this recognizance isn't discovered, communications are kept as covert as possible. They do this in several ways.

They may operate within existing encrypted tunnels or appear as just another regular operating service or application running within the background. VMware's research shows that on Linux-based multi-cloud environments, implant activities are performed as routine cron jobs, which are job schedulers. These allow Linux, macOS, and Unix environments to schedule processes to be run at regular intervals. These can include restarting the implant at regular timeframes, and this will help increase the implant's persistence.

That persistence is used to move laterally within the environment. During lateral movement, the attackers find other vulnerable systems and install more implants to increase their endurance and ability to move deeper within the environment. The attackers will also seek troves of valuable data and systems with high access levels. This can go on for weeks and months.

Not all implants are designed as malicious tools. Sometimes, as is the case with Cobalt Strike, they are used by security teams to help better secure their environments.

Linux-based attack management tools

Attack management tools are dual-use attack tools, as they can be helpful to both attackers and defenders alike. These tools provide the ability to discover networked assets, gain unauthorized access, and conduct command-and-control communications. One such tool is Cobalt Strike. Essentially, Cobalt Strike enables enterprise security teams to simulate actual attacks on their systems. Cobalt Strike uses an implant named Beacon that communicates back and gathers tasks to execute. However, attackers have also found Cobalt Strike's rich toolset and capabilities valuable.

Attackers have found Cobalt Strike so valuable that they have taken its implant (Beacon) and reimplemented it as a Linux-based Vermilion Strike. Vermilion Strike is a Linux-based RAT that uses the Cobalt Strike back end, the same protocols, structure, data formats, and will communicate with actual Cobalt Strike C2 servers. This is why attackers can take Cobalt Strike and deploy it in their environment, host it, and expand the systems they target to Linux systems using the Vermilion Strike beacon.

"Vermilion Strike is a big focus of this, and so that's how we got into this idea of tracking these different RATs," says Baskin.

As was noted in VMware's report, Vermilion Strike appears to be the first reimplementation of the Cobalt Strike protocol in the wild.

> "We have to focus on how payloads actually get into place. They will use that one compromised machine to jump to the next machine. They will enumerate all the resources within environments, such as the operating systems and vulnerabilities, and then use whatever exploits they can to move around."
>
> *– Brian Baskin, technical lead, Threat Analysis Unit at VMware*

"Because Cobalt Strike is such a ubiquitous threat on Windows, its expansion to other operating systems, such as Linux, is notable. It demonstrates the desire of threat actors to use readily available remote-control tools to target as many platforms as possible," the VMware researchers wrote.

The ability for enterprises to detect RATs is essential to successfully defend their

networks. RATs such as Vermilion Strike are commonly employed early in the attack lifecycle as they add more malware into the victim environment. VMware researchers have determined that a healthy combination of NDR software and EDR solutions can help stop these attacks before they get started.

Conclusion: Mitigating the risks

VMware recommends that organizations view their security program as an integral part of their operations and business

> "Because Cobalt Strike is such a ubiquitous threat on Windows, its expansion to other operating systems, such as Linux, is notable. It demonstrates the desire of threat actors to use readily available remote-control tools to target as many platforms as possible."
>
> – *VMware researchers*

environment. Protecting multi-cloud environments from RATs and other forms of malware and malicious attacks begins with visibility into workloads with comprehensive system context so that security and technical teams can easily prioritize their mitigations.

According to VMware, this requires an EDR solution that can monitor the actions performed by processes on cloud workloads and implement effective segmentation to contain risks. In addition, organizations need an NDR system that can recognize network-based evidence of attacks and malicious lateral movements to ideally block the malware before it can take hold of the target hosts.

Additionally, to adequately protect cloud systems, VMware advises that all workload access and communications must be secured, both within specific clouds and from cloud to cloud. Additionally, to stop attackers from moving laterally within the environment quickly, a zero-trust strategy should be in place so that users, devices, workloads, and networks are correctly and continuously vetted.

Finally, just as ransomware, crypto-jacking, and RATs have moved to Linux systems and place multi-cloud environments at risk — more malware is likely to target Linux operating systems. Defending against this threat requires a robust security program based on best practices and good in-depth defense, including securing the underlying infrastructure.

This means delivering security as a built-in distributed service across your control points of users, devices, workloads and networks.

Increasingly, this will include effective data backup and recovery process and EDR and NDR capabilities.

Since threat actors are increasingly targeting Linux and multi-cloud systems, it's imperative enterprises increasingly do what they can to secure them. ■

For more information about ebooks from SC Media, *please contact Bill Brenner, VP, content strategy, at bill.brenner@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact Dave Kaye, chief revenue officer, at (917) 613-8460, or via email at dave.kaye@cyberriskalliance.com.

Sponsor

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control.

With VMware Cross-Cloud™ services and our global ecosystem of partners, we deliver the smartest path to cloud, edge and app modernization. Our technology also supports multi-cloud autonomy for developers and consistent operations for DevSecOps—while creating a more secure, frictionless experience for the distributed workforce.

As the trusted foundation to accelerate innovation, VMware preserves customer choice and protects against lock-in. Instead of tradeoffs and compromise, our software offers businesses the freedom and flexibility they need to build the future.

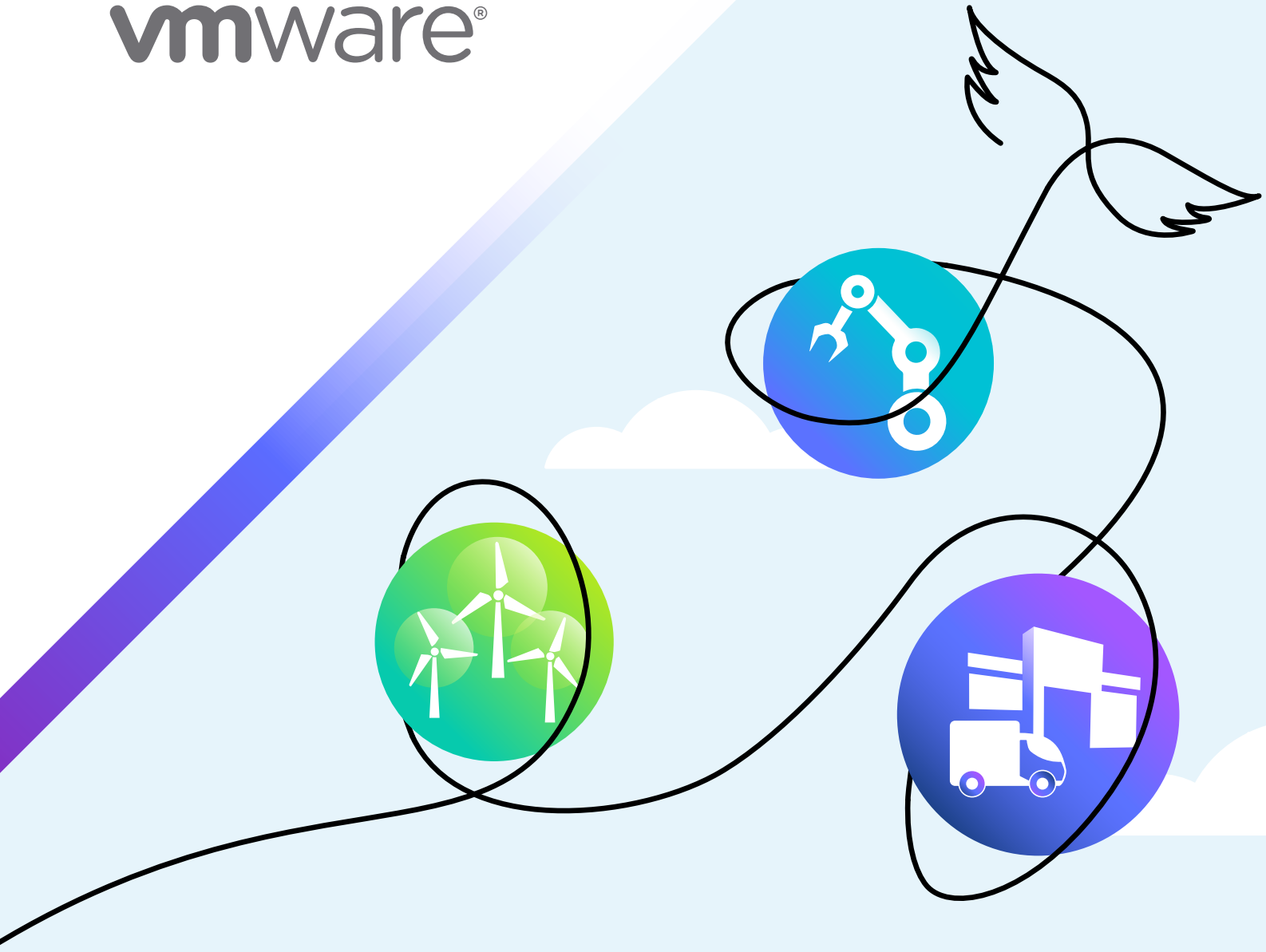
Learn more at www.vmware.com.

Masthead

EDITORIAL
VP, CONTENT STRATEGY
Bill Brenner
bill.brenner@cyberriskalliance.com
PROJECT MANAGER
Victor Thomas
victor.thomas@cyberriskalliance.com

SALES
CHIEF REVENUE OFFICER
Dave Kaye
(917) 613-8460 *dave.kaye@cyberriskalliance.com*
DIRECTOR, STRATEGIC ACCOUNTS
Valerie Williamson
(510)-900-0952 *valerie.williamson@cyberriskalliance.com*

vmware®



Secure your network. Free your business.

Accelerate innovation with VMware.

LEARN MORE